NUI Galway
OÉ Gaillimh

Semester Two Examinations 2016/2017

Exam Code(s)	4BCT1, 1MECE1
Exam(s)	Year 4 BSC in Computing Science and Information Technology, Masters in Electronic and Computer Engineering
Module Code(s)	CT437
Module(s)	Computer Security and Forensic Computing
Paper No.	1
Repeat Paper	No
External Examiner(s)	Dr. J. Power
Internal Examiner(s)	Dr. M. Schukat *Dr. C. Mulvihill

Instructions: Answer any 3 questions.
All questions will be marked equally.

Duration	2 hours
No. of Pages	3
Discipline(s)	Information Technology
Course Co-ordinator(s)	Dr. D. Chambers

Requirements:

Release in Exam Venue	Yes	X	No	
MCQ	Yes		No	X
Handout	None			
Statistical/ Log Tables	None			
Cambridge Tables	None			
Graph Paper	None			
Log Graph Paper	None			
Other Materials	None			
Graphic material in colour	Yes		No	X

PTO

1 (a) Entity authentication schemes often require some evidence of freshness in a communication, and this evidence is typically provided by nonces, clock-based mechanisms or sequence numbers. Explain briefly what is meant by the three terms ‘nonces’, ‘clock-based mechanisms’ and ‘sequence numbers’ in the context of supplying evidence of freshness (9 marks)

(b) Apart from freshness, entity authentication schemes should establish evidence of identity. A zero-knowledge scheme should allow a prover to convince a verifier of the identity of the prover without enabling the verifier to later impersonate the prover. Using any analogy of your own choosing, sketch at a high level how such a scheme might operate (8 marks)

(c) Consider a simple protocol for checking on the ‘liveness’ of Alice that involves the exchange of two messages. Bob, the checker, sends a message CHECK to Alice that contains a nonce and a query. Alice’s reply contains the message CHECK and a Message Authentication Code computed on the message CHECK. Find any one flaw in this scheme for Bob’s checking on the ‘liveness’ of Alice, and suggest how the flaw might be addressed (8 marks)

2 (a) In the context of scientific evidence, the so-called ‘Daubert’ criteria list four things that should be considered in order to have confidence that evidence supplied by some investigative technique is reliable. In your view how do these criteria impact on mobile forensic investigations? (8 marks)

(b) You are an IT officer for an organisation that is subject to considerable regulatory oversight and that has subscribed to very strict policies on information leakage. In the course of a routine examination of a laptop that was issued to a member of a team working on a recent case, you have found artefacts that indicate that a steganographic program was once present on the machine. Discuss whether in your view this discovery warrants further investigation, sketch what procedure you might follow if it does, and in the alternative sketch how you would close your examination if it does not (9 marks)

(c) Outline any two challenges that you think face digital forensics through the emergence of the ‘Internet of Things’ (8 marks)

3
Consider the document ‘Framework for Improving Critical Infrastructure Cybersecurity’, released by the National Institute of Standards and Technology (NIST) as draft version 1.1 in January 2017. The framework presented in this document is, as stated in the document, a ‘risk-based approach to managing cybersecurity risk’. Give your understanding of this framework under the three headings ‘Framework Core’ (9 marks), ‘Framework Implementation Tiers’ (8 marks) and ‘Framework Profile’ (8 marks).

4 (a) ‘A hash function is associated with notions of data integrity’. Give three security properties that a hash function should satisfy, and briefly indicate any one application area where in your view such security properties are needed (9 marks)

(b) Message Authentication Codes differ from a hash function in that they employ a shared key and a hash function (as such) has no key. From a security perspective, what, if anything, does a message authentication code offer that a hash function does not in your view? (8 marks)

(c) In one public-key digital signature scheme that provides for data origin authentication and non-repudiation, the hash of a long message M is signed and then the message and the hash are sent to the receiver. Suppose that a new scheme is proposed where a message M is decomposed into two small sub-units M1 and M2 and that M1 and M2 are individually signed and sent to the receiver. It is suggested that this is a better scheme in that it does not need a hash function. Is this proposed new scheme vulnerable in a way that the hashed scheme isn’t in your view? (8 marks)

5 (a) By considering the plaintext ‘010101’ and an associated key ‘111111’, explain the principle underlying encryption and decryption for a simple stream cipher that depends on a randomly generated keystream and XOR (8 marks)

(b) ‘Block ciphers work on blocks rather than bits’. With the aid of a diagram, show one encryption round for either a generic Feistel cipher or the AES block cipher (8 marks)

(c) Consider a security solution that provides a confidentiality service via a block cipher deployed in Cipher Block Chain (CBC) mode and also an integrity service delivered via so-called ‘CBC-MAC’. Discuss whether this scheme is vulnerable to a Message Authentication Code (MAC) forgery attack if the same key is used for both the confidentiality service and the integrity service. You may assume that a message consists of N blocks and that an attacker has changed all enciphered blocks apart from the last one (9 marks)

6 (a) In the context of a public key encryption scheme such as RSA, explain what is meant by the terms ‘private key’, ‘public key’ and ‘digital certificate’ (9 marks)

(b) Apart from specialised attacks, an encryption scheme such as RSA depends in general on the assumed ‘hardness’ of certain problems which are believed to give rise to ‘one-way’ functions. Briefly outline any two such problems that RSA relies on, explaining the term ‘one-way function’ in the course of your answer (8 marks)

(c) Public key schemes such as RSA are often deployed as so-called ‘hybrid encryption’ schemes, with the public key element being used to transfer a symmetric key which is subsequently used for general message encryption. By considering a long message that is to pass from Alice to Bob, briefly sketch how such a hybrid encryption scheme might operate (8 marks)